REMARKS

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 were pending at the time of the Office Action.

Claims 1, 2, 10, 11, 12, 16, 21, 24, 26, 31, 38, 40, 49, 52, 53, and 58 are amended.

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-50, 52-58, and 60-61 remain pending.

Applicants respectfully requests reconsideration and allowance of subject application.

Applicants appreciate the Examiner taking the time to speak with their attorney regarding the Office Action.

Summary of Interview

The Examiner was kind enough to host an in-person interview with applicants' attorney on February 6, 2007. The Examiner and applicants' attorney discussed a proposed amendment to the independent claims that would have applied the limitation that the client's ticket granting ticket was withheld from a server. Applicant's attorney noted that the asserted anticipatory reference described the server holding the client's ticket granting ticket. The Examiner indicated that, because the cited reference noted that the key to decrypt the client's ticket granting ticket was withheld from server, the client's ticket granting ticket was effectively withheld from the server. The Examiner invited applicants to articulate another way of describing the client's constraining of delegation to distinguish over the cited reference.

Applicants respectfully disagree with the Examiner's assertion that the asserted anticipatory reference discloses the withholding of the client's ticket granting ticket from the server when the reference expressly teaches the proxy receiving and holding the client's ticket granting ticket. Although applicants advance and emphasize other distinctions in this response, applicants' focus on these other distinctions should not be regarded as assent to the Examiner's position that the reference teaches or suggests the withholding of the client's ticket granting ticket from the server, when the cited reference teaches just the opposite.

Claim Rejections under 35 U.S.C. § 102

Claims 1-2, 4-17, 19-27, 29-35, 38-41, 43-46, 48-55, 57-58, and 60-61 are rejected under 35 U.S.C. § 102(b) as being anticipated by Fox et al., "Security on the Move: Indirect Authentication Using Kerberos" (1996) (hereinafter "Fox"). Applicants respectfully traverse the rejection.

In the interest of reducing the number of issues for the Examiner to consider in this response, the following discussion focuses on independent Claims 1, 12, 16, 26, 31, 38, 40, 49, and 58. The patentability of each remaining dependent claim is not necessarily separately addressed in detail. However, applicants' decision not to discuss the differences between the cited art and each dependent claim should not be considered as an admission that applicants concur with the Examiner's conclusion that these dependent claims are not patentable over the disclosure in the cited references. Similarly, applicants' decision not to discuss differences between the prior art and every claim element, or every comment made by the Examiner, should not be considered as an admission that applicants concur with the Examiner's interpretation and assertions regarding those claims. Indeed, applicants believe that all of the dependent claims patentably distinguish over the references cited. Moreover, a specific traverse of the rejection of each dependent claim is not required, since dependent claims are patentable for at least the same reasons as the independent claims from which the dependent claims ultimately depend.

As an introduction, applicants reference the specification of the present case which describes the context in which the invention was made and some of the problems which it addresses. The specification of the subject application addresses the problem of unconstrained forward target delegation. Generally, the user logon for a computer and the user authentication for network access control are two separate procedures. Nevertheless, to minimize the burden on a user in dealing with the different access control schemes, the user logon and the user authentication for network access are sometimes performed together. For example, in the case where the user authentication is implemented under the Kerberos protocol, when the user logs on the computer, the computer may also initiate a Kerberos authentication process. In the authentication process, the computer contacts a Kerberos Key Distribution Center (KDC) to first obtain a ticket granting ticket (TGT) for the user. The computer can then use the TGT to obtain from the KDC, a session ticket for itself.

As networks have evolved, there has been a trend to have multiple tiers of server/service computers arranged to handle client computer requests. A simple example is a client computer making a request to a World Wide Web website via the Internet. Here, there may be a front-end web server that handles the formatting and associated business rules of the request, and a back-end server that manages a database for the website. For additional security, the web site may be configured such that an authentication protocol forwards (or delegates) credentials, such as, e.g., the user's TGT, and/or possibly other information from the front-end server to a back-end server. This practice is becoming increasingly common in many websites, and/or other multiple-tiered networks.

Thus, any server/computer in possession of the user's TGT and associated authenticator can request tickets on behalf of the user/client from the KDC. This capability is currently used to provide forwarded ticket delegation. Unfortunately, such delegation to a server is essentially unconstrained for the life of the TGT.

Against this background, applicants respectfully assert that the claims are not anticipated by Fox. The claims of the present application recite constraining delegation of credentials. By contrast, as explained below, Fox sidesteps the problem of unconstrained delegation by not allowing such delegation.

Fox does not teach or suggest delegation. According to Fox, any credential the client needs, either for the client's own use or for a proxy to use on the client's behalf, is both requested by the client and delivered to the client. The requests may pass through a proxy, but the client never delegates to its proxy authority to request for credentials itself. In fact, the only credential given to the proxy that allows the proxy to act on the client's behalf is a service ticket that the client itself requests, decrypts, and then supplies to the proxy, as described below.

Figure 1 of Fox, which applicants have recreated below, shows that Fox's every request for a credential both originates with the client and ends with the credential being delivered to the client. By way of comparison, Figure 1(a) illustrates operation of the unmodified Kerberos protocol in which a client interacts directly with a trusted third party and a service the client wishes to access. At 1, *the client requests* an authentication credential or TGT. At 2, the KDC issues the TGT *to the client*. At 3, *the client uses its TGT to request a service ticket* from the ticket granting service (TGS) to access a server. At 4, *the TGS issues the service ticket to the client*. At 5, *the client presents the service ticket to the service*. At 6, the service responds to

the client. Thus, in conventional Kerberos, the client requests its own authentication and service credentials, and the requested authentication and service credentials are delivered to the client.

Fox's Figures 1(b)-1(d) and accompanying text on page 158 describe Fox's proxied implementation of Kerberos, in which a proxy is inserted between the client and other Kerberos resources. Fox describes the proxy as "an intelligent router." (Fox, Page157, Column 1, Paragraph 3). However, despite the inclusion of the proxy, the client is involved in every request for every service credential, just as in the case of unmodified Kerberos, and every credential the client requests is delivered to the client. Accordingly, Fox's proxy indeed does act merely as a "router" for passing the credentials, and the client does not delegate any of its authority to the proxy.
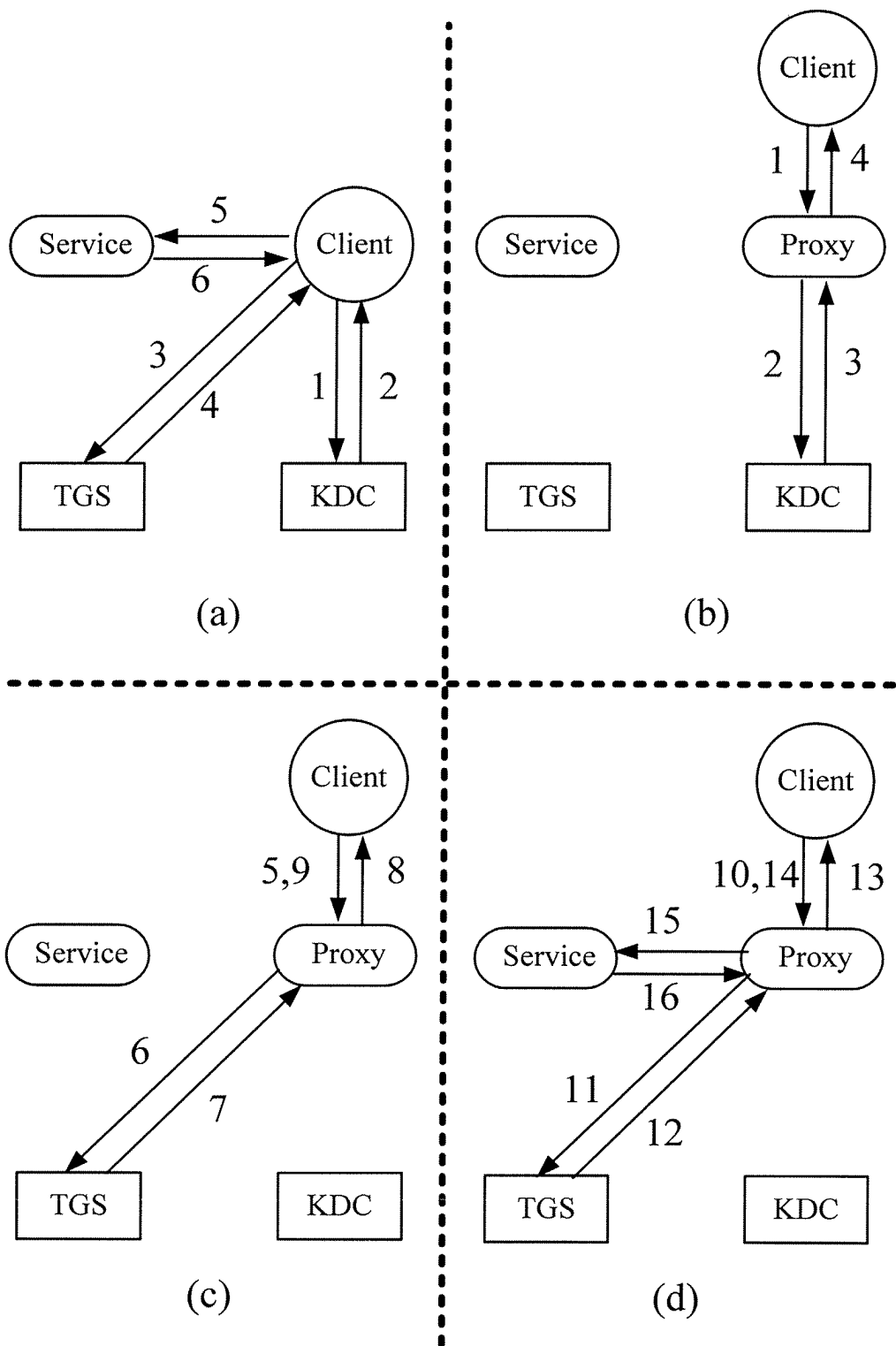
Figure 1 of Fox, from Page 157 of the reference.

In Fox's terminology, Figures 1(b) and 1(c) illustrate a "handshake phase," during which credentials are obtained to facilitate the eventual "service access phase" described in Figure 1(d). Applicants wish to emphasize two aspects of Fox that illustrate the distinction between Fox and what is recited by claim 1.

First, in Fox's handshake phase illustrated in Figures 1(b) and 1(c), *all requests and responses require the client's participation*. All the messages pass through the proxy in Fox's implementation, but all the requests for authentication and service ultimately are transacted by the client and the KDC or TGS.

Referring to Figure 1(b), at 1, *the client initiates a request for authentication*. At 2, the request is passed by the proxy to the KDC. At 3, the KDC issues a TGT and sends it to the proxy. However, Fox makes clear that the proxy is just a stopover for the TGT: "[t]he proxy possesses only the contents of message 3 above (the encrypted TGT packet); in particular, it cannot decrypt message 3 (since it does not know [the client's key] KC), and therefore it cannot possess [the key to client's TGT] $K_{c,tgs}$." Put another way, as noted by the Examiner in the most recent interview, Fox effectively withholds the TGT from the proxy, because the key needed to decrypt and use the TGT is never provided to the proxy. Thus, proxy is just a conduit through which the TGT passes to the client. At 4, *the TGT is delivered to the client*.

Similarly, in the second portion of the handshake phase illustrated in Figure 1(c), all requests and responses also pass from the client to the TGS and back to the client, with the proxy only acting as a conduit. At 5, *the client requests a service ticket to access the proxy*. At 6, the proxy passes the request to the TGS. At 7, the TGS passes the service ticket back to the proxy. At 8, *the proxy passes the service ticket back to the client*. It should be noted that the proxy does nothing with the service ticket received at 7 except to pass it to the client. It is only at 9, after the *client* has requested a service ticket for the client, received the service ticket, and decrypted the service ticket, that the service ticket is made available to the proxy when, at 9, *the client presents the service ticket to the proxy*. Fox thus describes a process in which the client is involved in every request and every other communication to obtain a service credential for the proxy.

Second, just as in its handshake phase, in Fox's service phase, the client is inextricably involved in every step of obtaining a credential. Figure 1(d) of Fox shows how its proxy obtains a service ticket to access the Service (which can be analogized to the target service recited in the

claims). As Fox states *"messages 10 through 14 in figure 1(d) (. . . are identical to messages 5 through 9 but with the proxy service P replaced by the appropriate service name)."* As previously described in recounting Fox's handshake phase, messages 5 through 9 in figure 1(c) *all are initiated or received by the client.* Similarly, messages 10 through 14 also *all originate and end with the client.* Thus, neither Fox's handshake phase nor its service access phase disclose anything about delegation, because Fox's client handles all of its own requests for authentication and service credentials.

It is only after the client has directly arranged all the service tickets that the proxy can engage a service on the client's behalf in the last two messages of figure 1(d) at messages 15 and 16. As specifically shown in figure 1(d), at 10, *the client requests the service ticket* for the proxy to access the Service. At 13, *the service ticket is returned to the client.* The proxy cannot make use of this service ticket until, at 14, *the client decrypts the proxy's service ticket and supplies it to the proxy for use.* Again, the client itself obtains all the authentications and service tickets for the proxy to engage the server on the client's behalf. The proxy is unable to obtain any service tickets without relaying messages back and forth to the client, thus, Fox does not teach delegation.

To further demonstrate the contrast between Fox and the pending claims, applicants present Figure 2 of the present application on the next page. The figure is offered by way of illustration, not limitation. In marked contrast to Fox, Figure 2 of the present application shows a server, acting on behalf of the client, requesting and obtaining its own service ticket, without the client having to request the service ticket or the service ticket necessarily being delivered to the client to decrypt the service ticket for the server to be able to use it.

As is explained in the specification and shown in Fig. 2, once the client 202 has been authenticated, it receives a service ticket 226 to access Server A 210. If the target service is not present on Server A 210, but instead is provided by Server B 212 or Server C 214, Server A 210 communicates directly with the trusted third party 204 to obtain a new service ticket 230 to access the target service on the client's behalf. The new service ticket 230 enables Server A 210 to access Server B 212 or Server C 214 for the client 202. As shown in Figure 2, Server A 210 can issue a request for a new service credential 230 without having to have the client 202 request a new service ticket 232 for itself. Thus, in the implementation exemplified in Figure 2, the client 202 delegates to Server A 210 the ability to request service tickets on behalf of the client.
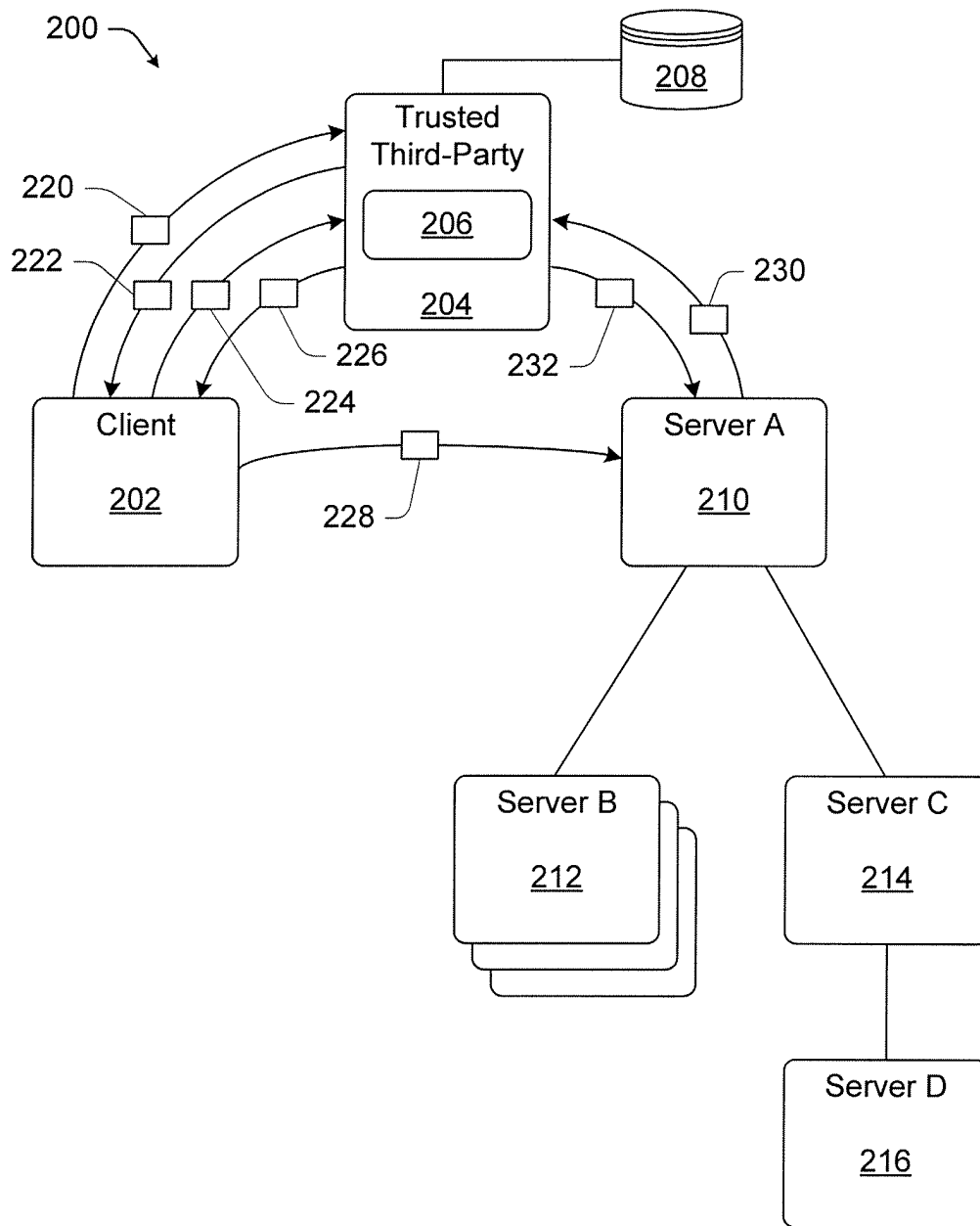
Figure 2 of the present application

Applicants emphasize elements 230 and 232 of Fig. 2. At 230, Server A 210 requests a service ticket from the Trusted Third Party 206. At 232, the Trusted Third Party 204 issues a service credential to Server A 210 to access one of the other servers 212-216 on behalf of the client. Note that, as shown in Fig. 2, the request for the service credential at 230 originates with Server A 210, not with Client 202 as in the process described by Fox. Furthermore, at 232, the

resulting service credential is issued to Server A 210 to access one of the other servers 212-216 *without* the service credential first delivering the service credential to Client 202 to have it decoded for Server A 210 to use it. Respectfully, Fig. 2 shows what Fox fails to teach or suggest: delegation to the server of the ability to request and use a service credential on behalf of the client, without the client having to request, receive, and decrypt all those credentials.

Turning to the claims, applicants respectfully submit that each of the pending claims is patentably distinguishable over Fox.

Claims 1, 2, and 4-11

Claim 1 as amended is presented here without indication of insertions or deletions for the sake of clarity:

> 1.   (Currently Amended) A method for constraining delegation by a client to a server, comprising:
>   identifying a target service to which access is sought on behalf of a client;
>   causing a server operatively coupled to the client to request a new service credential to access the target service on behalf of the client from a trusted third-party without providing a client's authentication credentials, wherein the server provides the trusted third-party with a credential authenticating the server, information about the target service, and a service credential previously provided by the client to the server allowing the client to access the server; and
>   causing the trusted third-party to provide the server with the new service credential that authorizes the server to access the target service on behalf of the client when one of:
>   the service credential specifies that delegation of the service credential is authorized; and
>   the trusted third-party maintains an indication that the delegation of the service credential is authorized.

Applicants submit that Fox fails to teach each of the elements recited by claim 1. Thus, Fox fails to anticipate claim 1 and its rejection under 35 U.S.C. § 102(b) should be withdrawn.

Claim 1 recites "causing a server operatively coupled to the client to request a new service credential to access the target service on behalf of the client from a trusted third-party." Again, using Fox, *the client must initiate its own request for a new service credential.* By contrast, claim 1 expressly recites "causing the trusted third-party to provide the server with the new service credential that authorizes the server to access the target service on behalf of the client." Fox describes the trusted third party *providing the client with a new service credential*

to access the target service, which the client can then decrypt and provide to the proxy. On the other hand, claim 1 recites allowing "the trusted third-party to provide the server with a new service credential." As previously explained, Fox's client requests all of the credentials, including any credential it may procure for a server, and if it does request a credential for a server, the client first must receive the credential, decrypt the credential, and deliver the credential to the proxy. Thus, Fox neither teaches nor suggests what is recited in claim 1. Accordingly, applicants submit that the rejection under 35 U.S.C. § 102(b) predicated on Fox must be withdrawn against claim 1.

Furthermore, Fox fails to describe how delegation can be controlled as recited in claim 1 as amended. Claim 1 recites:

> "causing the trusted third-party to provide the server with the new service credential that authorizes the server to access the target service on behalf of the client when one of:
>
>> the service credential specifies that the client authorizes delegation of the service credential; and
>>
>> the trusted third-party maintains an indication that the client authorizes the delegation of the service credential.

Respectfully, nothing in Fox describes the possibility of the service credential that allows the client to access the server to specify whether delegation is authorized, or of the trusted third party maintaining an indication that the client authorizes delegation of the service credential. Respectfully, Fox neither teaches nor suggests what is recited in claim 1. Applicants submit that the rejection under 35 U.S.C. § 102(b) predicated on Fox must be withdrawn against claim 1.

Claims 2 and 4-11 depend from and apply additional limitations to claim 1. Accordingly, claims 2 and 4-11 are patentable for at least the same reasons as claim 1 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 2 and 4-11.

In sum, applicants submit that claims 1, 2, and 4-11 are allowable over Fox.

Claims 12-15

Claim 12 as amended is reprinted below for the convenience of the Examiner:

12.   (Currently Amended) A method for constraining ~~the scope of authentication credential~~ delegation by a client to a server, comprising:

identifying a target service to which access is sought on behalf of a client; and

causing a server operatively coupled to the client to request <u>a new service credential to</u> access to the target service on behalf of the client[[,]] from a trusted third-party <u>without providing a client's authentication credentials</u>, wherein the server provides the trusted third-party with <u>an authentication</u> ~~a service~~ credential authenticating the server, information about the target service, and a service credential previously provided by the client <u>to the server</u> ~~for the service~~, and wherein the service credential previously provided by the client includes implementation-specific identity information constraining a scope of access delegated to the server; and

causing the trusted third-party to provide the server with a new service credential <u>that</u> ~~granted in the name of the client rather than the server such that the new service credential~~ authorizes the server to access the target service within the scope of access specified in the implementation-specific identity information.

Applicants incorporate their previous description of Fox. Again, applicants note that Fox fails to teach or suggest "causing a server . . . to request a new service credential." Fox fails to each or suggest the mechanism of constraining delegation of "causing the trusted third-party to provide the server with a new service credential that authorizes the server to access the target service within the scope of access specified in the implementation-specific identity information." Fox also fails to teach or suggest that causing the server to request a new service credential is possible "without providing the client's authentication credentials." Applicants respectfully assert that Fox fails to teach or suggest all of the elements recited by claim 12, and thus Fox cannot anticipate claim 12. Accordingly, applicants respectfully request that the rejection under 35 U.S.C. § 102(b) be withdrawn against claim 12.

Claims 13-15 depend from and apply additional limitations to claim 12. Accordingly, claims 13-15 are patentable for at least the same reasons as claim 12 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 13-15.

In sum, applicants submit that claims 13-15 are allowable over Fox.

Claim 16 is reprinted below for the convenience of the Examiner:

16.   (Currently Amended) A computer-readable medium having computer-executable instructions for performing tasks for constraining ~~a scope of~~ delegation by a client to a server, comprising:

in a server, determining a target service to which access is sought on behalf of a client coupled to the server; and

in the server, requesting a new service credential from a trusted third-party to access the target service without providing a client's authentication credentials by providing the trusted third-party with a credential authenticating the server, information about the target service, and a service credential that was previously provided to ~~associated with~~ the client and the requesting server such that issuance of the new service credential authorizes the server to access the service on behalf of the client ~~while within a scope of delegation authorized by the client~~ when one of:

the service credential specifies that the service credential is delegable; and

the trusted third-party maintains an indication that the service credential is delegable.

Applicants incorporate their previous description of Fox. Fox fails to teach or suggest "in the server, requesting a new service credential from a trusted third-party to access the target service." Moreover, because Fox does not describe delegation of access at all, Fox fails to each or suggest "that the issuance of the new service credential authorizes the server to access the service on behalf of the client while within a scope of delegation authorized by the client." Furthermore, as recited by claim 16 as amended, Fox fails to each or suggest the server being authorized to "access the service on behalf of the client when one of: the service credential specifies that the service credential is delegable; and the trusted third-party maintains an indication that the delegation of the service credential is delegable." Accordingly, applicants respectfully assert that Fox fails to teach or suggest all of the elements recited by claim 16, and thus Fox cannot anticipate claim 16.

Claims 17 and 19-25 depend from and apply additional limitations to claim 16. Accordingly, claims 17 and 19-25 are patentable for at least the same reasons as claim 16 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 17 and 19-25.

In sum, applicants submit that claims 16, 17, and 19-25 are allowable over Fox.

<u>Claims 26, 27, 29, and 30</u>

Claim 26 is reprinted below for the convenience of the Examiner:

26.   (Currently Amended) A system comprising:
a credential granting mechanism configured to receive a request for a new service credential from a server and in response generate the new service credential granted in the name of a client rather than the server if delegation is allowable and without providing a client's authentication credentials, and wherein the request includes:
a credential authenticating the requesting server,
identifying information about a target service to which access is sought on behalf of the client coupled to the server, and
a service credential that was previously granted to the client for use with the server and presenting a forwardable delegation flag indicating the client has authorized the delegation within a scope delegated by the client.

Applicants incorporate their previous description of Fox. Fox fails to teach or suggest "a credential granting mechanism configured to receive a request for a new service credential from a server and in response generate the new service credential granted in the name of a client rather than the server if delegation is allowable." Fox also fails to each or suggest authenticating the requesting server based on "a service credential that was previously granted to the client for use with the server and presenting a forwardable delegation flag indicating the client has authorized the delegation within a scope delegated by the client." Applicants respectfully assert that Fox fails to teach or suggest all of the elements recited by claim 26, and thus Fox cannot anticipate claim 26. Fox also fails to teach or suggest that a server requesting a new service credential is possible "without using the client's authentication credentials." Applicants respectfully assert that Fox fails to teach or suggest all of the elements recited by claim 26, and thus Fox cannot anticipate claim 26. Accordingly, applicants request that the rejection under 35 U.S.C. § 102(b) be withdrawn against claim 26.

Claims 27, 29, and 30 depend from and apply additional limitations to claim 26. Accordingly, claims 27, 29, and 30 are patentable for at least the same reasons as claim 26 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 27, 29, and 30.

In sum, applicants submit that claims 26, 27, 29, and 30 are allowable over Fox.

<u>Claims 31-35</u>

Claim 31 is reprinted below for the convenience of the Examiner:

31. (Currently Amended) A system for constraining ~~the scope of~~ delegation by a client to a server, comprising:

a server configured to generate a request for a new service credential in the name of a client rather than the server from a trusted third-party <u>without providing authentication credentials of the client</u>, the new service credential being associated with a client and a target service, the request comprising:

a credential authenticating the server,

information about the target service, and

a service credential associated with the client and the server

wherein the server is <u>allowed</u> ~~constrained~~ to access the target service <u>when one of:</u>

<u>the service credential specifies that the service credential is delegable; and</u>

<u>the trusted third-party maintains an indication that the service credential is delegable</u>.

Applicants incorporate their previous description of Fox. Fox fails to teach or suggest "a server configured to generate a request for a new service credential in the name of a client rather than the server from a trusted third-party." Furthermore, Fox fails to each or suggest allowing a server to access a target service "when one of: the service credential specifies that the client authorizes delegation of the service credential; and the trusted third-party maintains an indication that the client authorizes the delegation of the service credential." Fox also fails to teach or suggest that a server requesting a new service credential is possible "without using the authentication credentials of the client." Applicants respectfully assert that Fox fails to teach or suggest all of the elements recited by claim 31, and thus Fox cannot anticipate claim 31. Accordingly, applicants request that the rejection under 35 U.S.C. § 102(b) be withdrawn against claim 31.

Claims 32-35 depend from and apply additional limitations to claim 31. Accordingly, claims 32-35 are patentable for at least the same reasons as claim 31 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 32-35.

In sum, applicants submit that claims 31-35 are allowable over Fox.

Claim 38 is reprinted below for the convenience of the Examiner:

> 38.   (Currently Amended) A method comprising:
> separately authenticating a server and a client;
> providing the server with a server ticket granting ticket;
> providing the client with a client ticket granting ticket and a service ticket
> for use with the server;
> providing the server with the service ticket;
> in response to a request by the server, providing the server with a new
> service ticket ~~in an identity of the client rather than an identity of the server~~ for
> use by the server for use with a new service ~~while withholding from the server~~
> without requiring the server to have access to the client ticket granting ticket
> ~~thereby constraining delegation of the client ticket granting ticket~~ when one of:
> the service ticket specifies that the service credential is delegable;
> and
> the trusted third-party maintains an indication that the service
> credential is delegable.

Applicants incorporate their previous description of Fox. Applicants incorporate their previous description of Fox. Again, according to Fox, the client obtains all the tickets it needs, both for itself and for any node acting on its behalf. In addition, Fox fails to teach or suggest "providing the server with a server ticket granting ticket." Also, applicants maintain that Fox discloses the opposite of what is recited in claim 38, because Fox teaches providing the client's ticket granting ticket to the server, while claim 38 expressly recites that the client "withhold from the server the client ticket granting ticket." Respectfully, regardless of whether the server is provided with whatever it needs to decrypt or use the client's ticket granting ticket, Fox expressly discloses the divulging of the client ticket granting ticket to the server.

Moreover, Fox fails to describe providing the server with the new ticket "without requiring without requiring the server to have access to the client ticket granting ticket when one of: the service ticket specifies that the service credential is delegable; and the trusted third-party maintains an indication that the service credential is delegable." Applicants respectfully assert that Fox fails to teach or suggest all of the elements recited by claim 38, and thus Fox cannot anticipate claim 38. Accordingly, applicants request that the rejection under 35 U.S.C. § 102(b) be withdrawn against claim 38.

Claim 39 depends from and applies additional limitations to claim 38. Accordingly, claim 38 is patentable for at least the same reasons as claim 38 from which it depends. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 38-39.

Claims 40, 41, 43-46, and 48

Claim 40 is reprinted below for the convenience of the Examiner:

> 40.   (Currently Amended) A method for constraining a scope of delegation by a client to a server, comprising:
> identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;
> causing a server that is operatively coupled to the target service and the client to use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication protocol method; and
> causing the server to request from the second authentication method trusted third-party[[,]] a new service credential in an identity of the client rather than an identity of the server, for use by the server and the target service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with the credential authenticating the server to access the target service within a scope constrained by the client, information about the target service, and the service credential to itself; and
> causing the server to issue the new service credential when one of:
> the service credential to itself indicates it is delegable; and
> the second authentication method trusted third-party maintains an indication that the service credential to itself is delegable.

Applicants incorporate their previous description of Fox.

Fox fails to anticipate claim 40 for at least six reasons. First, applicants again note that Fox fails to teach or suggest "causing a server . . . to use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication protocol method," let alone causing the server to request anything because the client in Fox handles all of its own requests.

Second, Fox only contemplates the use of a single authentication method: Kerberos. Accordingly, Fox neither teaches nor suggests that the client may be authenticated using a first authentication method, while the server is authenticated using a second method.

Third, Fox neither teaches nor suggests causing the server to request a service credential to itself. Again, Fox only teaches a proxy forwarding requests for service credentials. Because every request for a service credential in Fox actually is initiated by the client itself, Fox fails to suggest causing a server to request anything for itself.

Fourth, Fox neither teaches nor suggests causing the server to use its own credential authenticating the server to obtain a service credential to itself. Again, every request for a service credential made by Fox comes from the client, and all such requests involve the client's own authentication credential.

Fifth, Fox fails to teach constraining delegation by only "causing the server to issue the new service credential when one of: the service credential to itself indicates it is delegable; and the second authentication method trusted third-party maintains an indication that the service credential to itself is delegable.

Sixth, Fox fails to teach constraining delegation by only "causing the server to issue the new service credential when one of: the service credential to itself indicates it is delegable; and the second authentication method trusted third-party maintains an indication that the service credential to itself is delegable." Thus, for at least these six reasons, applicants submit that Fox fails to teach or suggest what is recited by claim 40. Applicants respectfully request that the rejection under 35 U.S.C. § 102(b) be withdrawn against claim 40.

Claims 41, 43-46, and 48 depend from and apply additional limitations to claim 40. Accordingly, claims 41, 43-46, and 48 are patentable for at least the same reasons as claim 40 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 41, 43-46, and 48.

In sum, applicants submit that claims 40, 41, 43-46, and 48 are allowable over Fox.

<u>Claims 49, 50, 52-55, and 57</u>

Claim 49 is reprinted below for the convenience of the Examiner:

49. (Currently Amended) A computer-readable medium having computer-executable instructions for performing tasks for constraining a scope of delegation by a client to a server, comprising:

identifying a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method;

causing a server that is operatively coupled to the target service and the client <u>to use a credential authenticating the server</u> to request a service ticket to itself from a second authentication method trusted third-party by identifying the client and the first authentication method protocol; and

causing the server to request a new service ticket in an identity of the client rather than an identity of the server, for use by the server and the identified service, from the second authentication method trusted third-party, wherein the server provides the trusted third-party with <u>the credential</u> ticket authenticating the server to act within a scope of delegation permitted by the client, information about the target service, and the service ticket to itself; and

<u>causing the second authentication method trusted third-party to issue the new service ticket when one of:</u>

<u>the service ticket specifies the service ticket is delegable;</u> and

<u>the second authentication method trusted third-party maintains an indication that the service ticket is delegable.</u>

Applicants incorporate their previous description of Fox. Applicants incorporate their previous description of Fox. Again, applicants note that Fox fails to teach or suggest "causing a server . . . to request a service credential to itself," because clearly the client in Fox handles all of the requests for credentials, including requesting the service credential for the server to use. In addition, because Fox contemplates only a single authentication method – Kerberos – Fox does not and cannot anticipate causing the server to request a service ticket to itself "from a second authentication method trusted third-party by identifying the client and the first authentication method." Also, because the client in Fox handles all the requests for tickets, Fox also fails to teach the server providing "the trusted third party . . . with the service ticket to itself," because nothing in Fox teaches the trusted third party providing *anything* to the server itself.

In addition, Fox fails to teach or suggest "causing the second authentication method trusted third-party to issue the new service ticket when one of: the service ticket specifies the service ticket is delegable; and the second authentication method trusted third-party maintains an indication that the service ticket is delegable." Applicants respectfully assert that Fox fails to

teach or suggest all of the elements recited by claim 49, and thus Fox cannot anticipate claim 49. Accordingly, applicants request that the rejection under 35 U.S.C. § 102(b) be withdrawn against claim 49.

Claims 50, 52-55, and 57 depend from and apply additional limitations to claim 49. Accordingly, claims 50, 52-55, and 57 are patentable for at least the same reasons as claim 49 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 50, 52-55, and 57.

In sum, applicants submit that claims 49, 50, 52-55, and 57 are allowable over Fox.

Claims 58, 60, and 61

Claim 58 is reprinted below for the convenience of the Examiner:

58.   (Currently Amended) A system for constraining a scope of delegation by a client to a server, comprising:
a server configurable to:
identify a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method and that has presented a client service ticket authorizing the client to access the server and specifying what authorization the client delegates to the server,
use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication method, and
subsequently request a new service credential, for use by the server and the target service, from the second authentication method trusted third-party,
wherein the server provides the second authentication method trusted third-party with a credential authenticating the server, information about the target service, and the service credential to itself in an identity of the client rather than the server such that a scope of delegation authorized by the client constrains access by the server to the target service as authorized by the client in the client service ticket.

Applicants incorporate their previous description of Fox. Again, Fox contemplates only Kerberos as a single authentication method, and thus it cannot anticipate claim 58 which recites both a first authentication method and a second authentication method. In addition, Fox fails to teach or suggest "a server configurable to: identify a target service to which access is sought on behalf of a client that has been authenticated using a first authentication method and that has presented a client service ticket authorizing the client to access the server and specifying what authorization the client delegates to the server." Moreover, Fox also fails to teach or suggest to

"use a credential authenticating the server to request a service credential to itself from a second authentication method trusted third-party by identifying the client and the first authentication method." Furthermore, Fox fails to teach or suggest "that a scope of delegation authorized by the client constrains access by the server to the target service as authorized by the client in the client service ticket." Applicants respectfully assert that Fox fails to teach or suggest all of the elements recited by claim 58, and thus Fox cannot anticipate claim 58. Accordingly, applicants request that the rejection under 35 U.S.C. § 102(b) be withdrawn against claim 58.

Claims 60 and 61 depend from and apply additional limitations to claim 58. Accordingly, claims 60 and 61 are patentable for at least the same reasons as claim 58 from which they depend. Applicants thus request that the rejection under 35 U.S.C. § 102(b) also be withdrawn against claims 60 and 61.

In sum, applicants submit that claims 58, 60, and 61 are allowable over Fox.

Claim Rejections under 35 U.S.C. § 103

Claims 47 and 56 once again rejected under 35 U.S.C. § 103(a) as being obvious over Fox in view of Freier et al., "The SSL Protocol Version 3.0" (November 18, 1996). Claims 47 and 56 depend from claims 40 and 59, respectively. Because dependent claims 47 and 56 are patentable for at least the same reasons as the claims from which they depend, and add additional limitations to those claims, applicants request that the rejection similarly be withdrawn from claims 47 and 56.
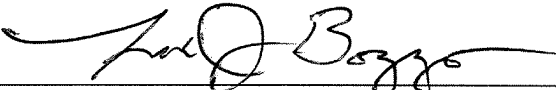
CONCLUSION

Claims 1-2, 4-17, 19-27, 29-36, 38-41, 43-50, 52-58, and 60-61 are in condition for

allowance. Applicants respectfully request entry of the amendment, consideration of the

foregoing remarks, and reconsideration and prompt allowance of the subject application. If any

issue remains unresolved that would prevent allowance of this case, the Examiner is requested to

contact the undersigned attorney to resolve the issue.

Respectfully submitted,

MERCHANT & GOULD P.C.
P.O. Box 2903
Minneapolis, Minnesota 55402-0903
(206) 342-6200

Date: June 29, 2007
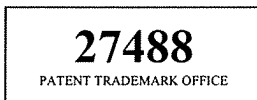
Frank J. Bozzo
Reg. No. 36,756
Direct Dial: (206) 342-6294

27488
PATENT TRADEMARK OFFICE